

# Dual-layer Digital Image Watermarking for Intellectual Property Right Protection

<sup>1</sup>Mr. H. E. Suryavanshi, <sup>2</sup>Prof. Amit Mishra and <sup>3</sup>Prof. Amit Sinhal

Department of Information Technology, Technocrats Institute of Technology, Bhopal, India

<sup>1</sup>hitendra.suryavanshi@gmail.com, <sup>2</sup>amitmishra.mtech@gmail.com and <sup>3</sup>amit\_sinhal@rediffmail.com

**Abstract:** Digital watermarking is a technique which is widely used in various application areas such as copyright protection, copy control, broadcast monitoring etc. In this paper a novel digital image watermarking technique is presented. To protect the intellectual property rights, two different watermarks are inserted in host image. The first watermark is used to monitor the any changes made in host image while second one is used as proof of ownership. The performance of proposed system is good and it withstands against various attacks such as Gaussian noise, salt and pepper, tampering etc.

**Keywords:** Digital Watermarking, Discrete Wavelet Transform, Fragile Watermark, LSB, Robustness.

## I. INTRODUCTION

Internet allows the public to exchange the information without any barriers. This information can be in the form of text, image, audio and video. The unrestricted access to information gives birth to some problems such as copyright violation, piracies etc. watermarking is a techniques developed to resolve these issues. Watermarking gains a lot of importance since last decade. It can be defined as a practice of undetectably modifying a work to embed a message about that work. Where work can be image, audio, video clip. [1]

In general, digital image watermarking system consist of two modules: embedder and extractor, as shown in Fig. 1. The embedder takes two inputs one is message which acts as watermark, and the other is host image in which we want to embed the message. The output of embedder is the watermarked image which can be stored for later use. Extraction module takes watermarked image and extracts the message. Most of the extraction modules only check whether image carries any watermark or not.

### A. Properties of Watermarking System

Watermarking system has number of properties and the importance of each property depends upon the type of applications and role that watermark plays. [2]

1) **Robustness:** The ability of the watermark to survive normal processing of content.

2) **Security:** The ability of the watermark to resist hostile attacks.

3) **Fidelity:** The perceptual quality of watermarked content.

4) **Data payload:** The amount of information that can be carried in awatermark.

### B. Classification of Watermarking

Watermarking can be classified into the number of types, as given below [3][4][5].

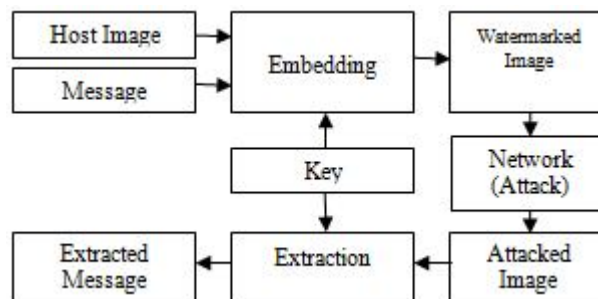


Fig. 1 General concept of watermarking

1) **Visible Watermarking:** The idea of visible watermark is very simple. The logos used in today's world everywhere is an example of visible watermark. They are especially used for conveying the immediate claim of ownership.

2) **Invisible Watermarking:** In this type of watermarking, rather than displaying logo, the information is concealed into the content itself.

3) **Fragile Watermarking:** Fragile watermarks have limited robustness. They are used to check whether any modification had taken place into the watermarked data.

**Public Watermarking:** These types of watermark are not secure 4) because they can read or viewed by anyone using specific algorithms.

## II. DISCRETE WAVELET TRANSFORM

Discrete wavelet transform is mathematical tool for hierarchically decomposing an image. Images are usually non-stationary two-dimensional signals and wavelet transform is effective in such case. When discrete wavelet transformation (DWT) applied on image, it decompose image into four frequency sub-bands (LL, HL, LH, HH) where LL refers to low pass band and other three sub-bands corresponds to horizontal (HL), vertical (LH) and diagonal (HH) high pass bands [6].

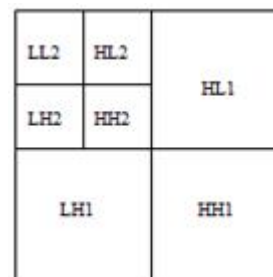


Fig.2 Two-level DWT decomposition

Fig. 2 shows two-level DWT decomposition of image. In

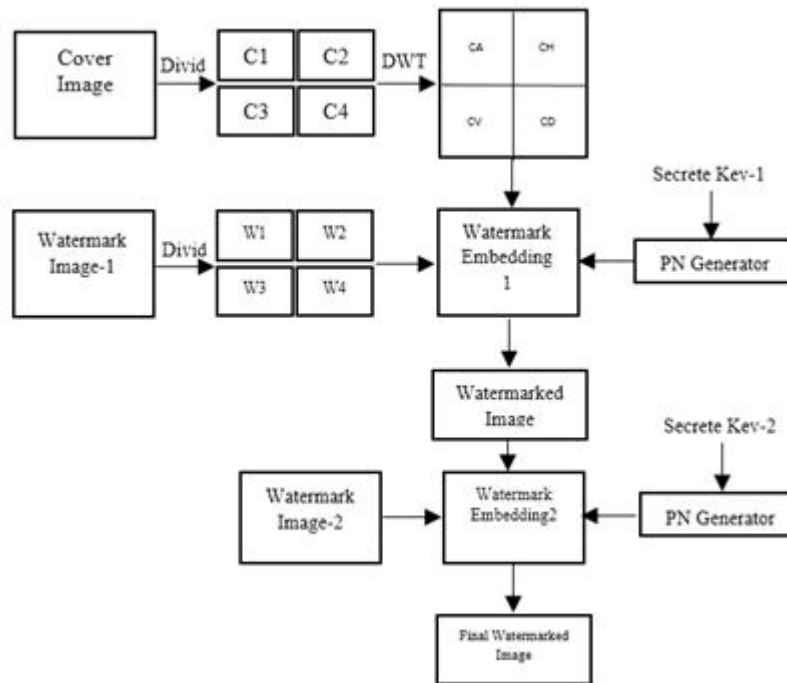


Fig.3 Proposed Watermarking Scheme

general, the watermark can be inserted into low frequency sub-bands (LL) because it increases the robustness of watermark but at the same time it may degrade the image significantly. High frequency bands (HH) contains edges and textures and changes that are caused due to watermark data inserted in such band cannot be noticed by human eye [7].

### III. PROPOSED WORK

In this section we present our proposed work. As illustrated in Fig. 3, the watermarking system consists of two embedders. The role of first embedder is to insert a watermark into an image by using wavelet transform. This watermark acts as robust watermark which cannot be removed from host image. Second embedder inserts watermark which acts as fragile watermark. This watermark is used to detect any alterations in an image. Single change in an image can be easily identified by using the second watermark. Spatial domain technique such as LSB replacement is used to insert the second watermark.

#### A. Watermark Insertion Method

1. Select the Original Image  $I_c [M_c, N_c]$  and Watermark Image  $W1 [M_w, N_w]$
2. Divide  $I_c$  and  $W1$  into four sections  $[I_1, I_2, I_3, I_4]$  and  $[W_1, W_2, W_3, W_4]$  by applying following equations

Part 1=Image  $(1:(x/2), 1:(y/2))$   
 Part 2=Image  $(1:(x/2), ((y/2)+1):y)$   
 Part 3=Image  $((x/2)+1:x, 1:(y/2))$   
 Part 4=Image  $((x/2)+1:x, ((y/2)+1):y)$

Where  $[x, y]$  = Size of the Image

3. Select the pair  $(I_i, W_i)$  where  $i=1, 2, 3, 4$  and repeat step no 4 to 13 for each pair
4. Apply DWT on  $I_i$  to get  $[CA, CH, CV, CD]$  coefficients

5. Convert  $W_i$  into binary watermark (contains 0s and 1s)
6. Resize  $W_i$  as  $W_i [1, M_w \times N_w]$
7. Set PN sequence generator using Secret Key-1
8. Repeat step 9 to 12 till  $(M_w \times N_w)$
9. Generate PN sequence
10. Calculate  $\beta$  factor as  $\beta = PN \times K$  where,  $k$  is robustness factor
11. Select the Coefficients  $[CH, CV]$
12. IF Watermark  $(W_i) = 1$   
 $C = C + \beta$   
 ELSE  
 $C = C$
13. Apply inverse DWT to get  $I_{wi}$
14. Collect all four section to get watermarked image ( $I_w$ )
15. Select the watermark image  $W2 [M_w, N_w]$
16. Resize  $W2$  to  $[M_c, N_c]$
17. Set PN sequence generator using Key-2
18. Repeat the step 19 to 20 till  $[M_c \times N_c]$
19. Randomly generate a number  $R$
20. IF  $R$  = Even Number  
 Set  $I_w$  (1st bit) to Watermark bit  
 ELSE  
 Set  $I_w$  (2nd bit) to Watermark bit
21. Final watermarked image ( $I_w$ ) is obtained
22. Stop

#### B. Watermark Extraction Method

1. Select the Watermarked Image  $I_w [M_w, N_w]$
2. Divide  $I_w$  into four sections  $[I_{w1}, I_{w2}, I_{w3}, I_{w4}]$  using same equations specified above
3. Create four dummy matrix  $[M_1, M_2, M_3, M_4]$  containing all zeros having size  $[M_w/2, N_w/2]$
4. for each  $(I_{wi}, M_i)$  pair repeat step 5 to 9 where  $i=1, 2, 3, 4$

5. Apply DWT on  $I_{wi}$  to get [WA, WH, WV, WD] coefficients
6. Set PN sequence generator using Key-1
7. Repeat step 8 till  $(M_w/2 \times N_w/2)$
8. Select [WH, WV] coefficients and calculate correlation
9. IF Correlation  $\geq$  Mean  
Set  $M_i=1$   
ELSE  
Set  $M_i=0$
10. Collect all  $M_i$  to get first watermark W1
11. Create a matrix W2 [ $M_w, N_w$ ]
12. Set PN sequence generator using Key-2
13. Repeat the step 14 to 16
14. Randomly generate a number R
15. IF R = Even Number  
Set W2 to  $I_w$  (1st bit)  
ELSE  
Set W2 to  $I_w$  (2nd bit)
16. Second watermark image (W2) is obtained
17. Stop

#### IV. RESULT ANALYSIS

This section presents the experimental results of the proposed digital image watermarking scheme. For the entire test in this paper MATLAB is used. The performance the proposed method is tested on 8-bit grayscale image of *baboon*, *Lena* and *peppers* of size  $512 \times 512$ . Fig 4. Shows the cover image and two watermarks that can be inserted into cover image.



Fig.4 (a) Baboon (b) Lena (c) Peppers (d) First watermark (e) Second watermark

The performance of the proposed watermarking technique is evaluated in terms of the invisibility and robustness. The PSNR (Peak-Signal-to-Noise Ratio) and MSE (Mean Square Error) are used to measure the quality of the watermarked image and attacked image. The PSNR is defined as follows [6] [7]:

$$PSNR = 10 \log_{10} \frac{I^2}{MSE}$$

Where,

$$MSE = \frac{1}{MN} \sum_{m,n} (I_{m,n} - I'_{m,n})^2$$

Where,  $I$  and  $I'$  are cover image and watermarked image. The normalized cross-correlation (NC) is used to check the quality of original and extracted watermark. [8]

$$NC = \frac{W \cdot W'}{\|W\| \cdot \|W'\|}$$

Where,  $W$  and  $W'$  are original and extracted watermarks.



Fig.5 (a) Original Image (b) After inserting first watermark (c) After inserting second watermark

Fig. 5 shows the original image of the baboon, the image after the insertion of first watermark and second watermark. The first watermark is inserted using blind watermarking technique. It is a robust watermark. The second watermark is a fragile watermark and embedded using LSB substitution technique. Its purpose is to detect tampering.

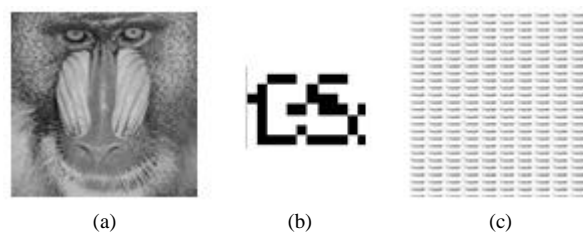


Fig.6 (a) Watermarked image (b) Extracted first watermark (c) Extracted second watermark

The robustness of the proposed watermarking scheme is tested against the various types of attacks such as, image tampering, Salt and pepper, Gaussian and Poisson. It is shown in the fig. 6 to 10.

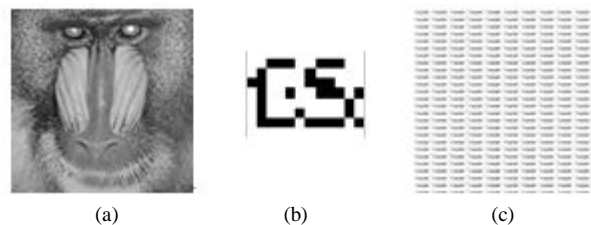


Fig. 7 (a) Attacked image (Tampering) (b) Extracted first watermark (c) Extracted second watermark

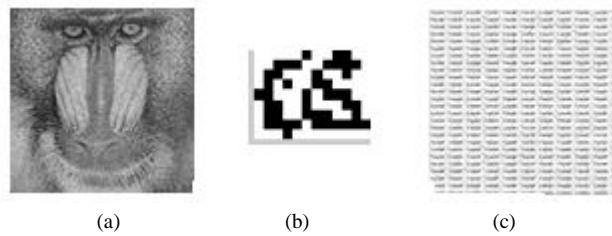


Fig. 8 (a) Attacked image (Salt & Pepper) (b) Extracted first watermark (c) Extracted second watermark

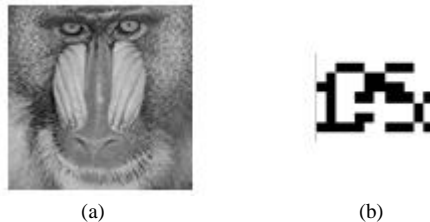


Fig. 9 (a) Attacked image (Gaussian Noise) (b) Extracted first watermark



Fig. 10 (a) Attacked image (Poisson) (b) Extracted first watermark

The performance of the system is shown in table 1 to 3 for different images such as Baboon, Lena and Peppers. For different values of K, robustness factor, different results are obtained as given in tables below.

TABLE I. PERFORMANCE OF WATERMARKING SYSTEM

K	Image-1: Babbon.bmp		
	PSNR	MSE	NC
0.1	38.6712	7.9527	0.5429
0.2	32.8323	31.5237	0.5968
0.3	29.4246	70.7842	0.6508
0.4	27.0669	125.7632	0.6952
0.5	25.1983	196.4499	0.7333
0.6	23.6141	282.9246	0.7651
0.7	22.2814	384.5371	0.7841
0.8	21.1269	501.6401	0.8190
0.9	20.1092	634.1065	0.8413
1.0	19.1963	782.4404	0.8603

TABLE II. PERFORMANCE OF WATERMARKING SYSTEM

K	Image-2: Lena.bmp		
	PSNR	MSE	NC
0.1	38.8532	7.9446	0.5841
0.2	33.0062	31.5301	0.6952
0.3	29.6291	70.8231	0.7651
0.4	27.1323	125.8479	0.8254
0.5	25.1939	196.6462	0.8730
0.6	23.6085	283.2924	0.8889
0.7	22.2732	385.2623	0.9270
0.8	21.1145	503.0735	0.9524
0.9	20.0935	636.4056	0.9651
1.0	19.1777	785.8025	0.9810

TABLE III. PERFORMANCE OF WATERMARKING SYSTEM

K	Image-3: Peppers.bmp		
	PSNR	MSE	NC
0.1	38.1598	7.9413	0.5175
0.2	32.3653	31.4904	0.6159
0.3	29.0096	70.5561	0.6952
0.4	26.7119	124.8649	0.7460
0.5	24.9696	194.2827	0.8032
0.6	23.5794	278.5260	0.8413
0.7	22.3656	377.1564	0.8857
0.8	21.2234	490.6154	0.9111
0.9	20.2171	618.5500	0.9429
1.0	19.3119	761.8840	0.9460

## CONCLUSIONS

In this paper a novel digital image watermarking technique is presented. This method is based on wavelet. The watermark is inserted using wavelet coefficient blocks. Watermark extraction process is independent on the original image. Watermarks can be extracted in any order. This scheme is tested against various attacks such as tampering, Gaussian noise. In the future, we will try to enhance our algorithm to obtain watermarked images with less distortion and to recover the watermark with good accuracy.

## ACKNOWLEDGMENT

The authors wish to thank Prof. Amit Mishra and Prof. Amit Sinhal for their valuable guidance.

## REFERENCES

- [1] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, "Digital watermarking and steganography", Second Edition, Morgan Kaufmann Publishers, 2007.
- [2] Husrev T. Sencar, Mahalingam Ramkumar, Ali N. Akansu, "Data hiding fundamentals and applications", Elsevier Academic Press, 2004.
- [3] Keshav S Rawat, Digital Watermarking Scheme for Authorization against Copying or Piracy of Color Images, Indian Journal of Computer Science and Engineering, Vol. 1, No. 4, 2010, pp. 295-300
- [4] Mohamed Abdulla Suhail, Digital watermarking for protection of intellectual property, (University of Bradford, UK, 2005)
- [5] Stefan Katzenbeisser, Fabien A. P. Petitcolas, Information hiding techniques for steganography and digital watermarking, Artech House Inc., 2000
- [6] Peining Tao and Ahmet M. Eskicioglu, A robust multiple watermarking scheme in the Discrete Wavelet Transformation Domain, Proc. SPIE 5601, Internet Multimedia Management Systems, Philadelphia, PA, 2004
- [7] Ali Al-Haj, "Combined DWT-DCT digital image watermarking", in Journal of Computer Science 3(9): 740-746, 2007, ISSN 1549-3636, © 2007 Science Publications
- [8] Hanaa A. Abdallah et. Al. "Blind wavelet-based image watermarking", in International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 4, No. 1, March 2011.